



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/853,835	05/10/2001	William Ray Cooley	P0367	6454
23735	7590	01/13/2006	EXAMINER	
DIGIMARC CORPORATION 9405 SW GEMINI DRIVE BEAVERTON, OR 97008			HA, LEYNNA A	
			ART UNIT	PAPER NUMBER
			2135	
DATE MAILED: 01/13/2006				

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary

Application No.

09/853,835

Applicant(s)

COOLEY ET AL.

Examiner

LEYNNA T. HA

Art Unit

2135

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --
Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

- 1) ☒ Responsive to communication(s) filed on 31 October 2005.
2a) ☒ This action is **FINAL**. 2b) ☐ This action is non-final.
3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

- 4) ☒ Claim(s) 1-27, 29-37 and 39-42 is/are pending in the application.
4a) Of the above claim(s) 28 and 38 is/are withdrawn from consideration.
5) ☐ Claim(s) _____ is/are allowed.
6) ☒ Claim(s) 1-27, 29-37 and 39-42 is/are rejected.
7) ☐ Claim(s) _____ is/are objected to.
8) ☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

- 9) ☐ The specification is objected to by the Examiner.
10) ☐ The drawing(s) filed on _____ is/are: a) ☐ accepted or b) ☐ objected to by the Examiner.
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

- 12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
a) ☐ All b) ☐ Some * c) ☐ None of:
1. ☐ Certified copies of the priority documents have been received.
2. ☐ Certified copies of the priority documents have been received in Application No. _____.
3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).
* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

- 1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)
Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

1. Claims 1-27 and 29-37 have been reexamined and are pending.

Claims 39-42 are new.

Claims 28 and 38 have been cancelled.

2. This is a Final rejection.

Claim Rejections - 35 USC § 102

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

A person shall be entitled to a patent unless –

(e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

3. **Claims 1-25 and 39-42 are rejected under 35 U.S.C. 102(e) as being anticipate by Venkatesan, et al. (US 6,801,999).**

Art Unit: 2135

As per claim 1:

Venkatesan, et al. discloses a method of regulating access to a website by a user terminal via the Internet, the user terminal reading a physical object including embedded steganographic indicia, said method comprising:

at the user terminal, extracting identifying data from the steganographic indicia, and providing the identifying data to a remotely located central computer;

[col.29, lines 46-50 and col.31, lines 62-65; As indicated in applicants specification steganographic is in the form of digital watermarking technology]

at the central computer:

identifying a pointer associated with the identifying data; **[col.5, lines 26-27]**

generating at least one component of response information; storing the response information; and **[col.28, lines 1-6 and col.29, lines 49-51]**

providing the pointer and response information to the user terminal; **[col.27, lines 55-58 and col.29, lines 52-56]**

at the user terminal, communicating with the website the pointer **[col.22, lines 6-20]** via and providing the response information to the website; **[col.5, lines 29-50 and col.30, line 11-17]**

at the website, communicating verification information to the central computer; and **[col.13, lines 37-38]**

at the central computer, verifying authority to access the website based at least in part on a comparison of the verification information **[col.28, lines 17-21]**

Art Unit: 2135

and the stored response information. [col.29, lines 1-8]

As per claim 2: See col.13, line 30 and col.14, lines 34-35; discussing the identifying data comprises an object identifier.

As per claim 3: See col.14, lines 26-27 and 29, lines 11-13; discussing the pointer comprises at least one of a URL, IP address and web address.

As per claim 4: See col.27, lines 10-14; discussing at least one component comprises a random number.

As per claim 5: See col.25, lines 18-22; discussing generating at least a second component, the second component comprising a time stamp.

As per claim 6: See col.25, lines 18-22 and col.27, lines 10-14; discussing the response information comprises at least the random number and the time stamp.

As per claim 7: See col.14, lines 34-35 and col.25, lines 18-22 and col.27, lines 10-14; discussing the verification information comprises at least the random number, the time stamp and a valid identifier.

As per claim 8: See col.14, lines 6-8 and col.23, line 9-12; discussing said verifying authority comprises indexing the stored response information via the communicated random number and determining whether the stored response information matches the valid identifier and whether the verification information is received within a predetermined time period.

As per claim 9: See col.11, lines 33-46; discussing when the stored response information matches the valid identifier within the predetermined time period, said method further comprising authorizing user terminal access to the

Art Unit: 2135

website.

As per claim 10: See col.17, lines 50-64; discussing when the stored response information does not match the valid identifier or the verification information is not received within the predetermined time period, said method further comprises signaling a lack of authority for the user terminal to access the website.

As per claim 11: See col.17, lines 50-64 and col.27, lines 11-16; discusses verifying authority comprises indexing the stored response information via the valid identifier and determining whether the stored random number matches the communicated random number, and whether the verification information is received within a predetermined time period.

As per claim 12: See col.14, line 15 and col.18, line 49; discusses encrypting at least one component of the of the response information.

As per claim 13: See col.17, lines 41-42 and 27, lines 10-13; discussing the document identifier is randomly generated.

As per claim 14:

Venkatesan teaches a method of authenticating permission to access a system comprising:

receiving a request to enter the system, the request including at least a verification key, the request being associated with at least a steganographically marked object; [col.27, lines 58-59 and col.29, lines 14-15 and 46-50; **As indicated in applicants specification steganographic is in the form of digital watermarking technology**]

Art Unit: 2135

querying a data structure to determine whether the verification key is authorized; and **[col.22, lines 32-43]**

allowing access to the system based on the response to the query.

[col.22, lines 55-60]

As per claim 15: See col.13, lines 57-58 and col.29, lines 11-13; discussing a website.

As per claim 16: See col.13, lines 57-58 and col.29, lines 11-13; discussing receiving comprises a user terminal signaling the website.

As per claim 17: See col.14, lines 10-15 and col.27, lines 10-13; discussing verification key comprises a first random number, and the data structure comprises at least one data record including a second random number and a first identifier.

As per claim 18: See col.17, lines 32-64; discussing the verification key further comprises a first time stamp and the data record further includes a second time stamp.

As per claim 19: See col.23, lines 10-25 and col.25, lines 18-22 and col.27, lines 10-14; discussing indexes the data record via the first random number, the first and second random numbers being equal, determines whether the first identifier matches the second identifier, and whether the first time stamp is within a predetermined time range based on the second time stamp, and signals to the system whether the first identifier matches the second identifier and whether the first time stamp is within the predetermined time range.

As per claim 20: See col.25, lines 7-8; discussing the first identifier comprises

Art Unit: 2135

an identifier extracted from a digital watermark.

As per claim 21: See col.23, lines 10-25 and col.25, lines 18-22 and col.27, lines 10-14; discussing indexes the data record via the second identifier, the first identifier and second identifier being equal, determines whether the first random number matches the second random number, and signals to the system whether the first random number matches the second random number and whether the verification information is received within a predetermined time.

As per claim 22:

Venkatesan discloses a system for exchanging data comprising:

a central server comprising at least one database [col.28, lines 1-6 and col.29, lines 49-51] including response information and pointer information [col.27, lines 55-58 and col.29, lines 52-56], wherein when a user terminal communicates an extracted watermark identifier to said central server [col.25, lines 5-11 and col.31, lines 62-65; **As indicated in applicants specification steganographic is in the form of digital watermarking technology**], said central server identifies a corresponding URL with the extracted watermark identifier [col.15, lines 47-58 and 23, lines 46-51], and wherein said central server generates a number[col.27, lines 5-15], and stores the number and extracted watermark identifier in the database as response information. [col.31, lines 58-65]

As per claim 23: See col.11, lines 39-45 and col.15, lines 51-52; discussing at least one database comprises a first database for storing pointers and a second database for storing response information.

Art Unit: 2135

As per claim 24: See col.25, lines 20-22; discussing server further generates a time stamp and stores the time stamp with the response information.

As per claim 25: See col.13, line 35 and col.25, lines 20-22; discussing the number comprises at least one of a random number, a pseudo-random number, and a predetermined number.

As per claim 39:

Venkatesan discloses a a method of regulating access to a website by a user device over a network, the user device reading an object including hidden steganographic indicia, said method comprising:

receiving identifying data extracted from hidden steganographic indicia, wherein the identifying data was extracted by a remotely located user device and communicated via a network; **[col.29, lines 46-50 and col.31, lines 62-65; As indicated in applicants specification steganographic is in the form of digital watermarking technology]**

identifying a pointer associated with the identifying data **[col.5, lines 26-27]**, the pointer comprising information to access a website; **[col.27, lines 55-58 and col.29, lines 52-56]**

providing at least one component of response information; storing the response information; **[col.28, lines 1-6 and col.29, lines 49-51]**

communicating the pointer and response information to the user device via the network **[col.22, lines 6-20]**, whereby the user device may access the website using at least the pointer and provide the response information to the website; **[col.5, lines 29-50 and col.30, line 11-17]**

Art Unit: 2135

receiving verification information from the website including at least a portion of the response information; **[col.28, lines 17-21]**

verifying authority to access the website based at least in part on a comparison of at least a portion of the verification information and at least a portion of the stored response information; and **[col.29, lines 1-8]**

providing an indication of authority to the website. **[col.28, lines 32-42]**

As per claim 40: See col.32, lines 38-39; discussing the indication inhibits access to the website.

As per claim 41: See col.6, lines 62-65; discussing the indication allows access to the website.

As per claim 42: See col.5, line 20; discussing the user device comprises a handheld device.

Claim Rejections - 35 USC § 102

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

A person shall be entitled to a patent unless –

(b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

4. Claims 26-27 and 29-37 are rejected under 35 U.S.C. 102(e) as being anticipate by Moskowitz, et al. (US 5,822,432).

As per claim 26:

Moskowitz teaches a method of operating a computer server, the computer server to communicate with at least one user terminal, said method comprising:

receiving an object identifier from the user terminal, wherein the object identifier is steganographically embedded in the object; **[col.9, lines 1-16 and 44-45; As indicated in applicants specification steganographic is in the form of digital watermarking technology where data are hidden (by embedding) in some other object]**

identifying a pointer associated with the document identifier **[col.6, lines 24-25]** wherein the pointer comprises at least one of a URL, IP address and web address; **[col.9, lines 29-39]**

generating at least one component of response information; **[col.9, lines 17-24]**

Art Unit: 2135

storing the response information; and [col.5, lines 35-39 and col.6, lines 25-40]

providing the pointer and response information to the user terminal. [col.9, lines 33-38]

As per claim 27: See col.3, lines 23-25; discussing the object identifier is steganographically embedded in the form of a digital watermark.

As per claim 28: **Cancelled**

As per claim 29: See col.6, lines 17-18; discussing the at least one component comprises a random number.

As per claim 30: See col.9, line 41; discussing the response information further comprises a time stamp.

As per claim 31: See col.6, lines 17-18 and col.9, line 41; discussing the response information comprises at least a random number and a time stamp.

As per claim 32: See col.6, lines 17-20 and col.9, lines 40-51; discussing verifying data, wherein said verifying data comprises indexing the stored response information via a second random number, and determining whether the stored document identifier matches a valid identifier.

As per claim 33: See col.9, lines 17-21 and 40-51; discussing when the stored document identifier matches the valid identifier, said method further comprises authorizing user terminal access.

As per claim 34: See col.3, lines 43-58 and col.9, lines 25-26; discussing when the stored document identifier does not match a valid identifier, said method further comprises signaling a lack of authority for the user terminal.

Art Unit: 2135

As per claim 35: See col.6, lines 17-20 and col.9, lines 40-51; discussing verifying data comprises indexing the stored response information via a valid identifier and determining whether the stored random number matches a second random number.

As per claim 36: See col.6, line 16-20; discussing encrypting at least one component of the response information.

As per claim 37: See col.3, line24-26; discussing the document identifier is randomly generated.

As per claim 38: **Cancelled**

Response to Arguments

5. *Applicant's arguments filed October 31,, 2005 have been fully considered but they are not persuasive.*

Applicant amended claims by replacing digital watermark with steganographic indicia where the examiner finds in the specification there are no distinction the two terms. According to the specification, "digital watermarking technology, a form of steganography... which digital data are hidden in some

Art Unit: 2135

other objects". Digital watermarks inherently embeds data for verification/authentication purposes which is hiding the data. Therefore, Moskowitz, et al. does teach embedded data exists in the digital watermark which is applicant's steganographic indicia.

Venkatesan teach the central server in the form of the Watermark Authority (WA) which is a third party wherein the WA is remotely located from the client PC and the Publisher (see FIG.15 and 16). Applicant's web site is disclosed in Venkatesan as the publisher that maintains a web server providing a web site (col.14, lines 26-28). Thus, the web site is referred hereinafter as the publisher. Hence, the WA accesses the publisher based at least in part on a comparison of the verification information (col.28, lines 17-21) and the stored response information (col.29, lines 1-8).

As per claim 14, recites requesting to enter the system, "the request including at least a verification key, the request being associated with at least a steganographically marked object" where the limitation merely receiving a request to enter a system which broadly leaves this limitation open to receiving at any system. Thus, receiving a request including a verification key to enter a system can broadly be given in light to either the publisher's system or the WA system of Venkatesan. Venkatesan discusses seeking to access the server (col.11, lines 26-30) to download the locked object wherein a request (col.29, lines 14-15 and col.33, lines 42-450) includes a file which contains a key for verification in order to access the object (col.14, lines 27-48). Further, Venkatesan discusses in the case of a media card, WA provides one key to a

Art Unit: 2135

card manufacturer where during manufacturing of the card, the key is embedded in encrypted form where the key is detects the presence of the corresponding one of the n watermarks in the protected objects (col.15, lines 15-18).

New claim 39 merely recites similar limitations to the combination of claims 1 and 14 where claim 39 goes more into details of the receiving identifying data.

As per claim 22, Venkatesan discusses the watermark having a value (identifier) that is extracted and sent from the user to compare to a value of the corresponding watermark stored in the object wherein the secret specifies a location (col.11, lines 40-46) or the address in terms of spatial domain key (col.13, lines 57-63) and is stored in the database as response information (col.33, lines 53-55). The identifier values can be the publisher ID (VID) and the product ID (PID) where these values from the watermark are extracted to determine a corresponding value (col.25, lines 5-11).

Claim 26 broadly recite "identifying a pointer associated with the object identifier, wherein the pointer comprises at least on of a URL, IP, and web address" where this limitation merely points to a location (i.e. URL, IP, address) of the object. The claim fails to limit pointing to a particular type of object and only recites an object identifier. The identifier for an object can be given its broadest and reasonable interpretation is data that identifies the object. Therefore, identifier of an object can be the watermark random generated key (col.1, lines 39-42) or the digital notary that contains a unique identification number (col.9, lines 40-49). Moskowitz discusses watermarks contain

Art Unit: 2135

information pertaining to geographical or electronic distribution restrictions or this information points to the URLs of online sites of the similar content. Moskowitz does teach "identifying a pointer associated with the document identifier [col.6, lines 24-25] wherein the pointer comprises at least one of a URL, IP address and web address; [col.9, lines 29-39]".

Conclusion

6. THIS ACTION IS MADE FINAL. Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to LEYNNA T. HA

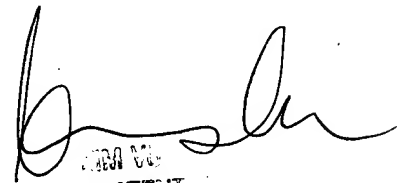
Art Unit: 2135

whose telephone number is (571) 272-3851. The examiner can normally be reached on Monday - Thursday (7:00 - 5:00PM).

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kim Vu can be reached on (571) 272-3859. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

LHa



KIM VU
PATENT
EXAMINER